# Протидія зростанню інтернет-шахрайств

Київська обласна державна адміністрація (Київська обласна військова адміністрація)
№4760/03/60.02/2023 від 16.05.2023
КЕП: БІЛЕЦЬКИЙ С. В. 16.05.2023
2B6C7DF9A3891DA1040000001863C1003F086E03
Сертифікат дійсний з 23.05.2022 до 23.05.2023 23:59

# Здійснення фінансових операцій через Інтернет

Захист від здійснення фінансових операцій через Інтернет є дуже важливою задачею для збереження вашого грошового майна та особистої інформації.

На наступних слайдах ви знайдете практичні поради щодо захисту від зловмисників в мережі Інтернет

# Здійснення фінансових операцій через Інтернет

## Поради по захисту

- Уникайте використання громадських Wi-Fi: Уникайте здійснення фінансових операцій через громадські Wi-Fi мережі, такі як кав'ярні або аеропорти. Ці мережі можуть бути небезпечними, оскільки зловмисники можуть перехоплювати ваші дані.
- Використовуйте надійні паролі: Встановіть складний пароль, який містить букви, цифри та символи. Не використовуйте один і той же пароль для різних сайтів.
- Користуйтеся захистом: Використовуйте антивірусне програмне забезпечення та перевіряйте свої пристрої на наявність шкідливих програм.

# Здійснення фінансових операцій через Інтернет

## Поради по захисту

- Увімкніть брандмауер: Переконайтеся, що брандмауер на вашому комп'ютері або маршрутизаторі увімкнений. Брандмауер допомагає блокувати небажані підключення до вашої мережі та зменшує ризик злому.
- Встановіть двоетапну автентифікацію: Якщо ваш провайдер банківських послуг дозволяє, встановіть двоетапну автентифікацію для свого облікового запису, щоб захистити його від несанкціонованого доступу.
- Використовуйте безпечні сайти: Перевіряйте, що сайт, на який ви входите, має захищене з'єднання та користується протоколом HTTPS.

# Шахрайські (фішингові) повідомлення

Шахрайські повідомлення, відомі також як фішингові повідомлення, це вид шахрайства, в якому зловмисники намагаються отримати ваші особисті дані, фінансову інформацію або зламати ваші облікові записи, шляхом надсилання підроблених електронних листів, повідомлень у соціальних мережах, смс або дзвінків.

Основною метою фішингу є зловживання вашою довірою. Шахраї можуть використовувати різні підступні методи, щоб змусити вас розкрити конфіденційну інформацію, наприклад, вони можуть стверджувати, що вони представники банку, онлайн-сервісу або іншої довіреної організації.

# Шахрайські (фішингові) повідомлення

## Поради по захисту

- Не відповідайте на підозрілі повідомлення. Якщо вам приходить незнайоме повідомлення з проханням про надання конфіденційної інформації, негайно видаліть його або проігноруйте. Не надсилайте свої паролі, особисті дані, банківську інформацію.
- Не відкривайте файли, які ви не очікували. Якщо вам приходить файл або посилання від незнайомого відправника, не відкривайте його безпосередньо.
- Перевірте адресу відправника. Шахраї часто намагаються підміняти адресу відправника, щоб видатися довіреним джерелом. Зверніть увагу на будь-які малі відмінності в адресі, наприклад, на неправильно написане ім'я домену або на різні знаки пунктуації.

# Шахрайські (фішингові) повідомлення

## Поради по захисту

- Не розкривайте особисту інформацію: Ніколи не надавайте свої особисті дані, такі як номери банківських карт, номери соціального страхування або іншу конфіденційну інформацію по телефону. Справжня компанія чи організація не повинна запитувати такі дані по телефону без належної ідентифікації.
- Не переходьте за посиланнями або не встановлюйте невідомі програми. Це може бути спроба зламати ваш телефон або отримати ваші конфіденційні дані.

# Інтернет-шахрайство

Ось кілька кроків, які можна вжити для захисту себе від Інтернет-шахрайства:

- Двоетапна перевірка: Активуйте двоетапну перевірку (2FA) для своїх онлайн-акаунтів, де це можливо. Це додатковий шар безпеки, який вимагає підтвердження вашої особи через додатковий пристрій або код.
- Будьте обережні на соціальних мережах: Не розкривайте приватну інформацію про себе на публічних профілях соціальних мереж.
- Антивірусне програмне забезпечення та оновлення. Це допоможе виявити і запобігти шкідливим програмам або веб-сайтам.

# Шахрайство з надзвичайною ситуацією

Шахрайство з надзвичайною ситуацією є формою шахрайства, коли зловмисники намагаються скористатися страхом, побоюванням або потребою людей під час кризових ситуацій. Вони використовують ці ситуації, щоб викрасти гроші, особисту інформацію або заволодіти обліковими записами.

# Шахрайство з надзвичайною ситуацією

## Поради по захисту

Благодійність: Шахраї можуть стверджувати, що збирають кошти на благодійність для жертв природних катастроф, пандемії або інших кризових подій. Вони можуть звертатися до вас по телефону, електронній пошті або соціальних мережах і просити пожертвування. Будьте обережні та перевіряйте достовірність організації перед наданням коштів.

# Шахрайство з надзвичайною ситуацією

## Поради по захисту

Фальшиві повідомлення від офіційних органів: Зловмисники можуть відправляти електронні листи або смс, претендуючи на представників правоохоронних органів, уряду або міжнародних організацій. Вони можуть стверджувати, що ви стали жертвою злочину або повинні сплатити штраф. Ніколи не розголошуйте особисту інформацію або не переводьте гроші, не перевіривши автентичність повідомлення.